UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/644,689	08/19/2003	Gregory Gordon Rose	020682	6710

23696 7590 07/23/2007
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
DADA, BEEMNET W	
ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
07/23/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
nanm@qualcomm.com

ED

Office Action Summary	Application No.	Applicant(s)	
	10/644,689	ROSE ET AL.	
	Examiner	Art Unit	
	Beemnet W. Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 May 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on May 01, 2007. Claims 37-43 have been amended. Claims 1-53 are pending.

Response to Arguments

2. Applicant's arguments with respect to claim 1-53 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 1-53 are rejected under 35 U.S.C. 102(a) as being anticipated by Ekdahl et al. 'SNOW – a new stream cipher' Nov. 2001 (hereinafter Ekdahl).

5. As per claims 1, 27 and 37, Ekdahl teaches a method of generating key stream comprising:

applying a cryptographic function on input values selected from a first array of values to generate output values (i.e., R1, R2 of FSM, figures 1 and 2, section 2, a description of SNOW);

selecting mask values from a second array of values (i.e., LFSR, figure 1, section 2, a description of SNOW); and

combining the output values with the mask values to generate a key stream block for the key stream (i.e., combining the output of LFSR and FSM (R1,R2) to generate a running key, figure 1 and section 2, a description of SNOW);

wherein the first and second arrays are finite (i.e., figures 1, 2 and section 2, a description of SNOW).

6. As per claim 44, Ekdahl teaches an apparatus for generating a key stream comprising:

a linear feedback shift register (LFSR) configured to generate a first array of values, wherein the values of the first array correspond to the values of the LFSR states (i.e., R1, R2 of FSM, figures 1 and 2, section 2, a description of SNOW);

a nonlinear filter module configured to apply a cryptographic function on input values selected from the first array to generate output values (i.e., R1, R2 of FSM, figures 1 and 2, section 2, a description of SNOW); and

a combining module configured to combine the output values with mask values selected from a second array of values to generate a key stream block for the key stream (i.e., combining the output of LFSR and FSM (R1,R2) to generate a running key, figure 1 and section 2, a description of SNOW);

wherein the first and second arrays are finite (i.e., figures 1, 2 and section 2, a description of SNOW).

7. As per claims 2, 28, 38 and 45 Ekdahl further teaches the method further comprising generating the second array from the first array (figures 1, 2 and section 2, a description of SNOW).

8. As per claims 3 and 5, Ekdahl further teaches the method further comprising using a linear feedback shift register (LFSR) to generate the first array, wherein the values of the first array correspond to the values of the LFSR states (figures 1, 2 and section 2, a description of SNOW).

9. As per claim 4, Ekdahl further teaches the method further comprising clocking the LFSR to generate the second array (figures 1, 2 and section 2, a description of SNOW).

10. As per claim 6-8 and 29 Ekdahl further teaches the method further comprising:

applying the cryptographic function on updated input values selected from an updated first array of values to generate updated output values, selecting updated mask values from an updated second array of values, and combining output values with the updated mask values to generate a new key stream block for the key stream (figures 1, 2 and section 2, a description of SNOW).

11. As per claims 9, 30 and 46, Ekdahi further teaches the method wherein the number of input values and the number of output values are equal (figures 1, 2 and section 2, a description of SNOW).

12. As per claims 10 and 47 Ekdahi further teaches the method wherein the first and second array each comprises seventeen values (figures 1, 2 and section 2, a description of SNOW).

13. As per claims 11-26, 31-36 and 48-53 Ekdahi further teaches the method wherein each value comprises of one or more words and wherein each word comprises two or more bytes (figures 1, 2 and section 2, a description of SNOW).

14. As per claims 39-43, Ekdahi further teaches the medium further comprising: performing a byte-wise substitution of at least one byte of an input value to generate intermediate values, mixing at least two bytes of a primary intermediate values to generate a secondary value to generate the output values (figures 1, 2 and section 2, a description of SNOW).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100